PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/08 | A1

(11) International Publication Number: **WO 00/51286**

(43) International Publication Date: 31 August 2000 (31.08.00)

(21) International Application Number: PCT/US00/05098

(22) International Filing Date: 24 February 2000 (24.02.00)

(30) Priority Data:
09/259,135 26 February 1999 (26.02.99) US

(71) Applicant *(for all designated States except US)*: BITWISE DESIGNS, INC. [US/US]; 2165 Technology Drive, Riverside Technology Park, Schenectady, NY 12308 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BORROWMAN, Colin, D. [US/US]; 112 Mercer Avenue, Schenectady, NY 12303 (US).

(74) Agents: WINTRINGHAM, Drew, M. et al.; Chadbourne & Parke LLP, 30 Rockefeller Plaza, 31st Floor, New York, NY 10112 (US).

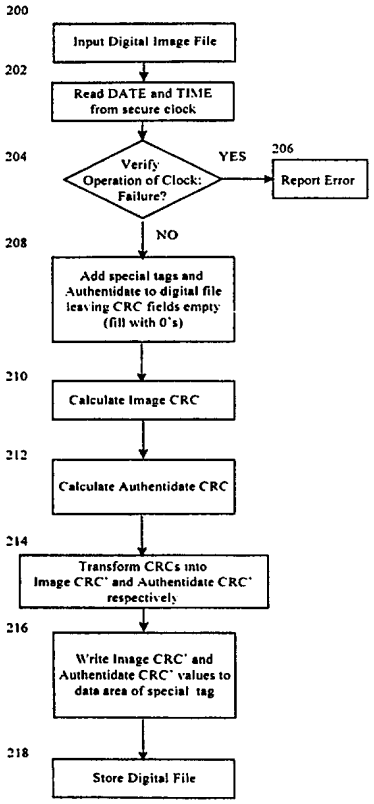
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DIGITAL FILE MANAGEMENT AND IMAGING SYSTEM AND METHOD INCLUDING SECURE FILE MARKING

(57) Abstract

A digital file management and imaging system records additional independent data with each stored image (200) including a true date gleaned from a secure clock (202) not settable by a user, a number derived from a cyclic redundancy code (CRC) algorithm for the image data (210) and the true date (212). This additional data is recorded within each digital file as soon as possible after the file is acquired. If the file is altered in any way after the recording of the additional data, recalculation of the image CRC on the altered file will not match the original image CRC recorded within it. Thus, the fact that it has been altered can be detected. Likewise, if the true date is altered in any way, recalculation of the date CRC will similarly reveal this fact.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

TITTLE OF THE INVENTION

Digital File Management And Imaging System And Method Including Secure File Marking

FIELD OF THE INVENTION

This invention relates generally to digital imaging systems and more particularly to digital file authentication.

BACKGROUND OF THE INVENTION

Digital imaging is the representation, and storage, of an image or object as a digital raster image. Digital imaging is increasingly used in many industries, partly because of the increased availability of enabling technology and partly due to the many advantages offered over conventional storage methods including: reduced storage space, increased access speed, focused retrievability (e.g., search capabilities), the ability to conveniently make "multiple" and "backup" copies of documents, and the ability to transfer or transmit documents quickly.

In the case of paper document originals, digital imaging systems will typically scan the paper document and store a representation of the scanned document as a digital raster image. An optical scanning device is typically used to scan images of the paper originals for storing as a digital image. The scanned images are exact representations of the original (limited only by the resolution limit of the scanning device), and can include handwriting, signatures, photos, figures, etc. Alternatively, digital images originating from digital cameras, medical imaging devices, or other sources may also be stored in a digital imaging system.

One drawback of known imaging technology is the inherent ability of digital images to be altered, for example, with a purpose to defraud. For example, although

an original paper document can be tampered with, such tampering (erasure or additions) will typically leave telltale evidence, digital images of those documents, on the other hand, can be perfectly altered leaving no such evidence. Thus, where the authenticity of an image is critical and may come into question (e.g., legal and medical fields), use of digital images is often not preferred, not acceptable or not admissible and therefore often avoided.

While many different digital image formats are available, in each case, the data is potentially alterable. Even if the digital imaging system does not explicitly provide an editing function, the images can be edited with a third party tool.

A proposed solution is the use of Write-Once, Read-Many ("WORM") optical media to store digital images. One advantage of WORM media storage is that the data it houses is inherently unalterable- data can be written only one time to the medium. However, this approach has several disadvantages as well. For example, data recorded on WORM media can be copied from the WORM disk of original recording to re-writable media, altered, and then recorded on new WORM disk with no traceability of such events.

Additionally, although it can be stated with great confidence that data on any one particular WORM disk has not been altered since it was recorded on that disk, the date and time when the data was recorded or whether the data matches an "original" of any kind cannot be determined with any certain or definitive means.

A known advance in file verification technology provides for registration of an "electronic signature" of a digital file (image, word processor document, audio or video clip, etc.). It is known to allow a user to locally select a file and locally run a program provided by a service provider to create an "electronic signature" of the

selected digital file based solely on file content. The signature along with a user-provided file name and user-selected keywords are uploaded to the provider's site and stored in a registration database maintained by the service provider under an account established for the particular user. One particular provider generates a "certificate of registration" showing, inter alia, the signature.

Verification of content and submittal date of the digital file at a later time requires going on-line to access the service provider's site and retrieving the prior registration record by file name or keywords. The retrieved database record shows the file signature and the original date that the file signature was registered. To complete verification, the user must run (locally again) the electronic signature program on the file to be verified and compare the regenerated signature to the retrieved registered signature to determine whether the signature of the digital file in question matches that of the originally registered file.

What the user now has is verification that the signature of the file in hand matches the signature of a file which was registered on a particular date.

SUMMARY AND OBJECTS OF THE INVENTION

The foregoing and other problems and deficiencies in image authentication in known digital imaging systems are solved and a technical advance is achieved by the present invention for providing digital file authentication by secure image marking.

In various aspects, it is among the objects of the present invention to provide a system and method for digital file management providing digital file authentication by secure file marking.

A digital file management system in one embodiment of the present invention comprises means for inputting a digital file and a secure date and time reference

providing date and time information. A date/time value is generated which is derived from the secure date and time information. An image value is derived from the digital file itself. The digital file is marked with the date and time information, the date/time value and the image value. The marked digital file is then stored.

Alternative embodiments can include such features as generating the date/time value and image value by a cyclic redundancy code algorithm and transforming the date/time value and image value via a mathematical transformation and marking the digital file with the transformed values.

In other embodiments, the secure date and time reference is a local secure clock.

In various embodiments, the digital file can be an image file, a text file or any other file format.

Alternative embodiments of the invention allow for inputting a digital image by way of an optical scanner for scanning an original image into a digital image or directly from digital cameras or medical imaging equipment. The marked digital file can also be stored in optical storage.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features and advantages of the present invention will become more apparent in light of the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawings, where

Fig. 1 illustrates a system implementation of the DocSTAR embodiment of the present invention;

Fig. 2 is a flow chart illustrating the file marking according to one embodiment of the present invention;

Fig. 3 is a flow chart illustrating validation of the CRCs in a filed marked image according to one embodiment of the present invention;

Fig. 4 is a flow chart illustrating one embodiment for setting the secure clock of the present invention;

Fig. 5 is a flow chart illustrating calculation of the Image CRC for TIFF format images according to one embodiment of the present invention;

Fig. 6 is a flow chart illustrating calculation of the Date CRC for TIFF format images according to one embodiment of the present invention;

Fig. 7 is a flow chart illustrating calculation of the Image CRC for JPEG format images according to one embodiment of the present invention; and

Fig. 8 is a flow chart illustrating calculation of the Date CRC for JPEG format images according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The following description of the present invention uses for illustrative purposes the Authentidate™ image authentication system incorporated in the turn-key document management and imaging system, DocSTAR™, both of which are available from BitWise Designs, Inc, the assignee of the present invention. While the DocSTAR embodiment of the present invention is geared towards storing, marking and authenticating paper document originals, any digital file can be processed by the method and system of the present invention as will be described. The following discussion with references to the DocSTAR embodiment are in no way intended to be limiting and are made for illustrative purposes only to facilitate explanation and understanding of the present invention.

Figure 1 illustrates an exemplary embodiment of the DocSTAR document management and imaging system implementation of the present invention.

A DocSTAR system host 100 is configured in communication with an input device 110, storage device 120 and a secure time and date reference 130.

In this embodiment, system host 100 is implemented as a IBM PC or workstation, input device 110 is an optical scanner, storage device 120 is an optical storage device and the secure time and date reference 130 is provided by a hardware key which incorporates a secure clock.

Original images will be scanned by optical scanner 110. The resulting digital image will be processed by system host 100 according to the method of the present invention which will be discussed in further detail herein, and then stored on optical storage device 120 from where it can be later retrieved.

The image authentication system of the present invention operates in one aspect by recording additional independent data with each stored digital file. These additional data includes: a "true date" which is gleaned from a secure clock (described in further detail below) which is not settable by the user (the Authentidate™); a number derived from a cyclic redundancy code (CRC) algorithm (described in further detail below) against the image data, this number is called the "image CRC"; and a CRC derived from the "true date", called the "date CRC".

These additional data is preferably recorded within each digital file as soon as possible after the image is acquired by the system (from, for example, scanner 110 in the DocSTAR embodiment). As will be discussed in further detail, if the image is altered in any way after the recording of the additional data, recalculation of the image CRC on the altered image will not match the original image CRC recorded within it.

Thus, the fact that the image has been altered or is otherwise compromised can be detected. Likewise, if the true date is altered in any way, recalculation of the date CRC will similarly reveal this fact.

The image and date CRCs can be checked and verified at any time. If the recalculated value matches the recorded value, it can be stated with extreme confidence that the image presently recorded was recorded on the specified date and has not been altered in any way since then. No other known system, including paper storage, can offer similar assurance as to the creation date or authenticity of a document.

With reference to Figure 2, the operation of the present invention will now be described.

Digital files are first acquired (either retrieved from storage or received from input device 110). (Step 200.) Date and time information is obtained from secure clock 130. (Step 202.) Proper operation of the secure clock is assessed. (Step 204.) If the secure clock is deemed functional, then the date and time data are accepted as read from the clock (in step 202). If a failure of the secure clock is determined, an error indication will be returned and the image processing is halted. (Step 206.) With the clock having been deemed functional (in step 204), special tags (as will be discussed infra) and the Authentidate information (including date and time) are added to the digital file and the CRC data fields are initialized to 0 (i.e., the data fields are filled with 0's). (Step 208.)

Two computed values are then calculated, which are derived from the image content and Authentidate information, respectively. The computed values can be computed in any fashion based on data contained within the digital file which will

allow detection of data corruption, such as for example, a standard checksum. In this embodiment of the present invention, cyclic redundancy codes ("CRC"), essentially a more complex checksum calculation, are used to derive the computed values. Any calculation method, however, is acceptable which will provide a number which is derived from the document content data and is suitable for detection of data corruption.

In this embodiment, the computed values are generated by a known CRC algorithm (which will be discussed in further detail below) which is run on both the image content and the Authentidate, creating an Image CRC and an Authentidate CRC, respectively. (Steps 210, 212.) The Image CRC and Authentidate CRC are "transformed" by a proprietary mathematical transformation for added security (as will be discussed infra) creating an Image CRC′ and an Authentidate CRC′. (Step 214.)

The image file is then marked with the Image CRC′ and Authentidate CRC′. (Step 216.) The marked digital files are stored on optical media by optical storage device 120. (Step 218.)

The authenticity of the image and the time and date stamp can then subsequently be determined by examining the computed values stored within the Digital Files as shown in Fig. 3 which depicts an exemplary flow chart describing one embodiment for validating CRCs in a filed image.

The first step in validating the CRCs in an digital file is to read the special tag and date areas and retrieve the stored image CRC and date CRC values. (Step 300.) If the CRC values cannot be located or read in the digital file (step 302), then, it is determined that either the image has not been properly filed or the image has been

altered or is otherwise compromised, and an error is posted. (Step 304.) If the special tags are found, the CRCs are recalculated for the digital file and the date string. (Step 306.) The same algorithms used to calculate the CRCs initially are used to regenerate them at this point. The recalculated image CRC is transformed and compared to the image CRC read from the tag. (Step 308.) (Alternatively, the stored image CRC can be reverse transform prior to comparison to the recalculated value.) If the recalculated digital file CRC does not match the one stored in the special tag, the image is determined to have been altered or otherwise be corrupted and an error is indicated. (Step 310.) If the stored and recalculated image CRCs compare favorably (i.e., they match), the date CRCs are tested. The recalculated date CRC is transformed and compared to the date CRC read from the tag. (Step 312.) (Alternatively, the stored date CRC can be reverse transformed prior to comparison with the recalculated value.) If the recalculated date CRC does not match the one stored in the special tag, the date string is determined to have been altered or be otherwise corrupted and an error is indicated. (Step 314.) If the date CRCs match, at this point both image and date CRCs have compared favorably, the digital file is determined to be unaltered and thus authenticated. (Step 316.)

As will be appreciated from the foregoing description, the use of a secure, non-compromisable clock is fundamental to the present invention. It serves as a secure time and date source which is not alterable by the user. The secure clock maintains the time and date even when the computer is turned off with the aid of a battery backup.

One could use either custom designed hardware or a commercially available product that offers a secure clock. In either case, a mechanism must be in place to prevent fraudulent or arbitrary date/time adjustment.

In the DocSTAR embodiment, a commercially available product that incorporates a secure clock into a physical hardware key is utilized (sometimes called a "dongle"). The hardware key connects to the computer's parallel port and can be accessed through an application programming interface (API) provided by the manufacturer.

The hardware key chosen for use in the DocSTAR embodiment of the present invention is the TIMEHASP-4 available from Aladdin Knowledge Systems, LTD. The security of the hardware key is protected by a custom ASIC chip (Application Specific Integrated Circuit), a unique set of passwords used only by the system provider (for example, BitWise Designs, Inc. the assignee hereof and a "provider" of the DocSTAR system) and advanced protection algorithms and anti-debugging technology in the manufacturer's programming interface and device drivers. This offers a high degree of security for the secure clock.

The current date and time are factory programmed into the secure clock contained within the hardware key during assembly of the DocSTAR Host computer. While any time setting may be used, the secure clock in this embodiment is set to Greenwich Mean Time (GMT) eliminating the need to adjust the clock for different local time zones or for daylight savings time.

A mechanism can be incorporated to make adjustments in the clock to reset or correct the clock for slight inaccuracies that can develop over time. For example, in one embodiment as illustrated in Figure 4, the date and time in the secure clock can be

changed by means of a special administration program resident on a user's system which will only allow changes to the secure date and time when the user supplies a proper authentication code supplied by the system provider, such as, for example, the Technical Support department of BitWise Designs, Inc., the assignee hereof. The authentication code will only work to change the secure clock date and time from its current date and time values to the current GMT maintained by the system provider. This prevents the user from altering the secure clock arbitrarily and thereby stamping images with an incorrect or fraudulent date and time.

In this embodiment, an authentication code is required to change the secure clock. To obtain this code, a support technician on the system provider system enters the Hardware Key serial number and the current secure clock date into a secured custom program (the "Eagle Call Tracking System") maintained at BitWise Designs, Inc. (step 400) which will generate an authentication code (step 402). The authentication code will allow the field technician or end user to change the secure clock only to the date and time established and maintained at BitWise Designs, Inc.

The authentication code in this embodiment is determined through a mathematical algorithm which yields one unique code given the current secure clock date, the hardware key serial number, and the desired change to date and time. This authentication code is of limited validity in that it will not work on another day in the future to reset the clock to the date and time on the day the authentication code was given.

The code is entered at the user end. (Step 404.) The desired clock setting is entered at the user end. (Step 406.) The administration program used on the client system allows a small time window (20 minutes) for which any time entered will

match the authentication code. Authentication codes are calculated internally for times 5 minutes before and 15 after the given change to time. If the given authentication code matches any of the codes within the time window, the authentication code is deemed correct and implemented. This will allow a field technician to account for several minutes delay while the authentication code is communicated.

Thus the desired setting is validated against the authentication code to determine whether the code will authenticate the date and time change requested. (Step 408.) If invalidity is determined, an error is returned and the clock is not updated. (Step 409.) With a valid request, the actual change to the secure clock will not occur until the Update Clock command is entered at the user end. (Step 410.) This allows a field technician to accurately synchronize the field clock with the clock maintained at BitWise Designs, Inc. After the Update Command is issued, the authentication code is re-validated against the clock information to ensure it is still valid. (Step 412.) If invalidity is determined, an error is returned and the clock is not updated. (Step 413.) The clock is updated. (Step 414.)

Alternatively, secure clocks can be reprogrammed by the service provider at the provider's facility (e.g., BitWise Designs, Inc.) by attaching the hardware key directly to a designated Eagle system at BitWise Designs, Inc. and issuing the update secure clock command. The hardware key serial number is verified and the secure clock date and time are updated to GMT date and time maintained at BitWise Designs, Inc.

In further alternative embodiments, clock adjustments to correct for inaccuracies that can develop over time or to set the clock can be implemented as an

automated process where a user can cause a clock update from a remote secure clock but the user cannot himself actually set the clock information.

Either the manual or automated method of clock setting and update described above will prevent the user from altering the secure clock arbitrarily and thereby stamping images with an incorrect or fraudulent date and time.

As can be expected within the limits of current available technology, the battery in each clock will eventually fail, or the clock can otherwise become defective over time. These conditions are tested by software prior to image processing to ensure that invalid dates from a defective clock (or dead battery) are not recorded in images, thus compromising the reliability of the image marking. In the event of a clock failure, image filing is disabled until the clock is repaired or replaced.

The computed values mentioned above with reference to Figure 2, in the DocSTAR embodiment of the present invention are Cyclic Redundancy Codes (CRCs). The CRC is a 32 bit-integer value which represents the result of performing the known CRC-32 algorithm on a block of data. The CRC-32 algorithm is a common, public domain algorithm for detecting even minute changes in data with a variety of applications. For example, CRCs are used in the communications field to verify that data has been transmitted correctly over transmission lines of unknown quality. It is also used to detect corruption of compressed data such as in the popular PKZIP utility. One of the strengths of CRCs is detecting changes to data which might otherwise go undetected. For example, if bit errors occur in a given block of data but their sum is coincidentally the same as that of the original data, this error might go undetected if a standard checksum were to be used. The CRC-32 algorithm would

detect this type of change because the resulting code is not simply a sum of the component data as in a standard checksum.

A technical discussion of the CRC-32 algorithm will not be presented here. There are many sources of CRC-32 algorithms and source code in the public domain. Sample C++ source code for a CRC32 algorithm which is implemented in the DocSTAR embodiment of the present invention, is shown below. As stated earlier, use of the CRC is not required for the present invention per se, and any calculation method is acceptable which will provide a number which is derived from the image data and is suitable for detection of data corruption. The exemplary C++ source code is shown here:

```
long  CRCTable[] =
      {
       0x00000000L,     0x77073096L,     0x0EE0E612CL,    0x990951BAL,
       0x076DC419L,     0x706AF48FL,     0x0E963A535L,    0x9E6495A3L,
       0x0EDB8832L,     0x79DCB8A4L,     0x0E0D5E91EL,    0x97D2D988L,
       0x09B64C2BL,     0x7EB17CBDL,     0x0E7B82D07L,    0x90BF1D91L,
       0x1DB71064L,     0x6AB020F2L,     0x0F3B97148L,    0x84BE41DEL,
       0x1ADAD47DL,     0x6DDDE4EBL,     0x0F4D4B551L,    0x83D385C7L,
       0x136C9856L,     0x646BA8C0L,     0x0FD62F97AL,    0x8A65C9ECL,
       0x14015C4FL,     0x63066CD9L,     0x0FA0F3D63L,    0x8D080DF5L,
       0x3B6E20C8L,     0x4C69105EL,     0x0D56041E4L,    0x0A2677172L,
       0x3C03E4D1L,     0x4B04D447L,     0x0D20D85FDL,    0x0A50AB56BL,
       0x35B5A8FAL,     0x42B2986CL,     0x0DBBBC9D6L,    0x0ACBCF940L,
       0x32D86CE3L,     0x45DF5C75L,     0x0DCD60DCFL,    0x0ABD13D59L,
       0x26D930ACL,     0x51DE003AL,     0x0C8D75180L,    0x0BFD06116L,
       0x21B4F4B5L,     0x56B3C423L,     0x0CFBA9599L,    0x0B8BDA50FL,
       0x2802B89EL,     0x5F058808L,     0x0C60CD9B2L,    0x0B10BE924L,
       0x2F6F7C87L,     0x58684C11L,     0x0C1611DABL,    0x0B6662D3DL,

       0x76DC4190L,     0x01DB7106L,     0x98D220BCL,     0x0EFD5102AL,
       0x71B18589L,     0x06B6B51FL,     0x9FBFE4A5L,     0x0E8B8D433L,
       0x7807C9A2L,     0x0F00F934L,     0x9609A88EL,     0x0E10E9818L,
       0x7F6A0DBBL,     0x086D3D2DL,     0x91646C97L,     0x0E6635C01L,
       0x6B6B51F4L,     0x1C6C6162L,     0x856530D8L,     0x0F262004EL,
       0x6C0695EDL,     0x1B01A57BL,     0x8208F4C1L,     0x0F50FC457L,
       0x65B0D9C6L,     0x12B7E950L,     0x8BBEB8EAL,     0x0FCB9887CL,
       0x62DD1DDFL,     0x15DA2D49L,     0x8CD37CF3L,     0x0FBD44C65L,
```

```
    0x4DB26158L,    0x3AB551CEL,    0x0A3BC0074L,   0x0D4BB30E2L,
    0x4ADFA541L,    0x3DD895D7L,    0x0A4D1C46DL,   0x0D3D6F4FBL,
    0x4369E96AL,    0x346ED9FCL,    0x0AD678846L,   0x0DA60B8D0L,
    0x44042D73L,    0x33031DE5L,    0x0AA0A4C5FL,   0x0DD0D7CC9L,
    0x5005713CL,    0x270241AAL,    0x0BE0B1010L,   0x0C90C2086L,
    0x5768B525L,    0x206F85B3L,    0x0B966D409L,   0x0CE61E49FL,
    0x5EDEF90EL,    0x29D9C998L,    0x0B0D09822L,   0x0C7D7A8B4L,
    0x59B33D17L,    0x2EB40D81L,    0x0B7BD5C3BL,   0x0C0BA6CADL,

    0x0EDB88320L,   0x9ABFB3B6L,    0x03B6E20CL,    0x74B1D29AL,
    0x0EAD54739L,   0x9DD277AFL,    0x04DB2615L,    0x73DC1683L,
    0x0E3630B12L,   0x94643B84L,    0x0D6D6A3EL     0x7A6A5AA8L,
    0x0E40ECF0BL,   0x9309FF9DL,    0x0A00AE27L,    0x7D079EB1L,
    0x0F00F9344L,   0x8708A3D2L,    0x1E01F268L,    0x6906C2FEL,
    0x0F762575DL,   0x806567CBL,    0x196C3671L,    0x6E6B06E7L,
    0x0FED41B76L,   0x89D32BE0L,    0x10DA7A5AL,    0x67DD4ACCL,
    0x0F9B9DF6FL,   0x8EBEEFF9L,    0x17B7BE43L,    0x60B08ED5L,
    0x0D6D6A3E8L,   0x0A1D1937EL,   0x38D8C2C4L,    0x4FDFF252L,
    0x0D1BB67F1L,   0x0A6BC5767L,   0x3FB506DDL,    0x48B2364BL,
    0x0D80D2BDAL,   0x0AF0A1B4CL,   0x36034AF6L,    0x41047A60L,
    0x0DF60EFC3L,   0x0A867DF55L,   0x316E8EEFL,    0x4669BE79L,
    0x0CB61B38CL,   0x0BC66831AL,   0x256FD2A0L,    0x5268E236L,
    0x0CC0C7795L,   0x0BB0B4703L,   0x220216B9L,    0x5505262FL,
    0x0C5BA3BBEL,   0x0B2BD0B28L,   0x2BB45A92L,    0x5CB36A04L,
    0x0C2D7FFA7L,   0x0B5D0CF31L,   0x2CD99E8BL,    0x5BDEAE1DL,

    0x9B64C2B0L,    0x0EC63F226L,   0x756AA39CL,    0x026D930AL,
    0x9C0906A9L,    0x0EB0E363FL,   0x72076785L,    0x05005713L,
    0x95BF4A82L,    0x0E2B87A14L,   0x7BB12BAEL,    0x0CB61B38L,
    0x92D28E9BL,    0x0E5D5BE0DL,   0x7CDCEFB7L     0x0BDBDF21L,
    0x86D3D2D4L,    0x0F1D4E242L,   0x68DDB3F8L,    0x1FDA836EL,
    0x81BE16CDL,    0x0F6B9265BL,   0x6FB077E1L,    0x18B74777L,
    0x88085AE6L,    0x0FF0F6A70L,   0x66063BCAL,    0x11010B5CL,
    0x8F659EFFL,    0x0F862AE69L,   0x616BFFD3L,    0x166CCF45L,
    0x0A00AE278L,   0x0D70DD2EEL,   0x4E048354L,    0x3903B3C2L,
    0x0A7672661L,   0x0D06016F7L,   0x4969474DL,    0x3E6E77DBL,
    0x0AED16A4AL,   0x0D9D65ADCL,   0x40DF0B66L,    0x37D83BF0L,
    0x0A9BCAE53L,   0x0DEBB9EC5L,   0x47B2CF7FL,    0x30B5FFE9L,
    0x0BDBDF21CL,   0x0CABAC28AL,   0x53B39330L,    0x24B4A3A6L,
    0x0BAD03605L,   0x0CDD70693L,   0x54DE5729L,    0x23D967BFL,
    0x0B3667A2EL,   0x0C4614AB8L,   0x5D681B02L,    0x2A6F2B94L,
    0x0B40BBE37L,   0x0C30C8EA1L,   0x5A05DF1BL,    0x2D02EF8DL

};

UINT32 CRCFileBlock(UINT16 hFile, UINT32 lOffset, UINT32 lLength, UINT32 lSeed)
{
    // calculate CRC on file block with seed given
    // use 0xFFFFFFFFL for initial seed
    // returns 0 on success, returns lSeed on error
```

```
        int ret;
        char buffer[COPYBUFFERLEN];
        UINT32 lRemainLength;
        UINT16 uBlockSize;
        UINT32 lSourceOff;
        UINT32 lCRC;
        UINT16 i, index;

        lCRC = lSeed;

        if(lLength > COPYBUFFERLEN)
                uBlockSize = COPYBUFFERLEN;
        else
                uBlockSize = (UINT16)lLength;

        lRemainLength = lLength;
        lSourceOff = lOffset;

        while(lRemainLength) {
                ret = ReadFileBlock(buffer, hFile, lSourceOff, uBlockSize);
                if(ret)
                        return lSeed;

                for (i=0; i<uBlockSize; i++) {
                        index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;
                        lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
                }
                lCRC = ~lCRC;

                lRemainLength -= uBlockSize;
                lSourceOff += uBlockSize;
                if(lRemainLength < uBlockSize)
                        uBlockSize = (UINT16)lRemainLength;
        }

        return lCRC;
}

UINT32 CRCBlock(char* buffer, UINT16 nLength, UINT32 lSeed)
{
        // calculate CRC on file block with seed given
        // use 0xFFFFFFFFL for initial seed
        // returns 0 on success, returns lSeed on error (ignores error)

        UINT32 lCRC;
        UINT16 i, index;

        lCRC = lSeed;

        for (i=0; i<nLength; i++) {
                index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;
```

```
            lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
        }
        lCRC = ~lCRC;
        return lCRC;
}
```

Sample C++ Source Code to Calculate CRC-32

While a CRC value alone may be used, a higher level of security can be incorporated into the present invention to ensure the authenticity of an image by addition of a mathematical transformation to the CRC value. As indicated, a typical algorithm to calculate a CRC-32 is in the public domain and thus easily accessible. This fact, in conjunction with the details provided herein, would allow anyone to recalculate the CRC on an altered image, enabling them to counterfeit an "Authentidate" and falsely confirm the image as authentic and unaltered. In the present invention, the actual calculated (image or date) CRC is mathematically transformed to a new value prior to image marking. The functional requirements of the transformation are that the resultant value for any input value is consistent, and that the resultant value is unique for each unique input value. The transformation could, for example, be a permutation of the bit-order of the input, an exclusive OR of the input value with a consistent, predetermined "magic" number, or a combination of these operations.

While the particular transformation technique implemented is not critical, it should be understood that the specific technique used to accomplish the transformation in the practice of this invention should remain confidential to the provider, i.e., a "proprietary transformation technique", as any disclosure or dissemination of the method would likely compromise system security and

effectiveness. To give a simple parallel, failure to safeguard the proprietary transformation technique would essentially be the equivalent of password protecting a file and then distributing the password.

Recording information in tags within digital files requires knowledge of the individual digital file formats and the standards governing the structure of their formats. These standards dictate how information will be stored in the file, in what order, using what compression algorithm, etc. Most digital file formats have provisions for accommodating storage of user data in the digital file in addition to the image data. The DocSTAR file management and imaging system embodiment of the present invention uses known TIFF (Tagged Image File)and JPEG (Joint Photographic Experts Group) file formats for storage of (scanned) bitonal and color images, respectively. The standards for TIFF and JPEG image file formats allow for inclusion of user data inside the image file in a manner which does not affect the displayed image. As will be readily understood, the present invention is equally applicable to other file formats which have a mechanism to store user-defined data in the file or the file marked with the user-defined data can be stored in an ancillary file or separate database, for example, for word processing documents, spreadsheets, digitized audio or video or any other digitized file.

The known TIFF format is a file format which allows image data to be stored in a compressed manner along with information about the image (tags) such as compression method used, resolution, size, number of colors, title, date, etc.

A written world-wide standard defines the TIFF file format, what tags must be present, what tags are optional and how specific tags are used. The maintaining organization of the TIFF standard, Adobe Corporation, accepts requests for custom

tag numbers for companies developing applications which use tags within the TIFF image. Adobe will assign unique numbers to individual companies to prevent interference between vendors. For example, BitWise Designs, Inc., the assignee hereof, applied for and was assigned its own proprietary tags numbers, other vendors will likewise be assigned their own unique proprietary tag numbers. Use of a custom tag allows storage of a custom data block. The TIFF specification calls for programs to ignore tags that they do not understand and which are not in the baseline specification. This allows common image viewers to view, display and print images which have custom tags because the image files still fit the TIFF specification.

In the case of TIFF image files, the following TIFF image tags are used:

Tag #	Use
10Dh	Document Name
10Eh	Image Description
132h	Date Time
9244h	BitWise DocSTAR Custom Tag 1 custom data block contains proprietary information including: Image CRC Authentidate CRC

Illustrated in Fig. 5 is an exemplary flow chart demonstrating calculation of an image CRC for a TIFF image file. The calculation of the image CRC for the TIFF image file calls for calculating a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to –1. (Step 500). The routine works through the format of the TIFF file based on the Image File Directory (IFD) for the file, calculating CRC-32 for each IFD entry and their associated data (step 502) passing results of the prior CRC-32 as the seed to the next (step 510) until all the IFD entries have been cycled through. (Step 506)

All tags and data areas are processed except the following tags and data areas (step 508):

Tag #	Description
0x010d	TIFFTAG_DOCUMENTNAME
0x010e	TIFFTAG_IMAGEDESCRIPTION
0x0132	TIFFTAG_DATETIME
0x9244	TIFFTAG_DOCSTARTAG1

After processing all IFD entries for the file (step 506), the proprietary transformation method (as described above) is used to transform the resulting CRC value into a unique and secure value CRC'. (Step 512.) The transformed image CRC value, CRC' is then stored in the image file. (Step 514.)

Illustrated in Fig. 6 is an exemplary flow chart demonstrating calculation of a date CRC for a TIFF image file. The calculation of the date CRC for the TIFF image file requires a routine which can calculate a CRC-32 on a given block of data using a given 32 bit seed value. The initial seed value is set to the image CRC value. (Step 600.) The routine reads the 0x0132 TIFFTAG_DATETIME tag. (Step 602.) If the DATETIME tag cannot be found and read (step 604), an error is returned (step 605), otherwise, a CRC-32 is calculated for the data contained within the DATE TIME tag. (Step 606.) The resulting CRC is then transformed into CRC' by means of the proprietary transformation technique (step 608) and stored within the image file. (Step 610.)

The Joint Photographic Experts Group developed the namesake format and maintains the standard for JPEG and the JPG file format (sometimes also called JFIF – JPEG File Image Format). This format was developed for the storage and transmission of photographic images. The compression techniques used are ideally suited to storing subtle differences between color changes, such as a photograph.

As is known, a JPG file is interpreted as a stream of characters with special identifiers called "markers" separating different elements of the image information and image data. The exact meaning of each marker is not important to this discussion except that the JPG standard defines a set of markers to be used by manufacturers for special or proprietary features. These markers are named "APPx" where x is a digit between 0 and 9 inclusive.

The present invention adds a special marker and data block to JPG files when they are stored. In this embodiment, the "APP8" marker will be used for the simple reason that this marker is rarely used by other manufacturers. This marker holds various proprietary information including the following:

Authentidate
Image CRC
Authentidate CRC

Illustrated in Fig. 7 is an exemplary flow chart demonstrating calculation of an image CRC for a JPEG image file. The calculation of the CRC for the JPEG image file requires a routine which can calculate a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to –1. (Step 700.) The image file data is read sequentially and the position of the APP8 is determined and read. (Step 702.) If the APP8 marker cannot be found and read (step 704), an error is returned. (Step 705.) A CRC-32 is calculated for all data in the file from the beginning of the file up to but not including the APP8 marker. (Step 706.) The result of this calculation is used as a seed to calculate a CRC-32 on the remainder of the file following the APP8 marker. (Step 708.) The resulting CRC is transformed into CRC' by means of the proprietary transformation technique. (Step 710.) The transformed image CRC' is then stored within the image file. (Step 712.)

Illustrated in Fig. 8 is an exemplary flow chart demonstrating calculation of a date CRCs for a JPEG image file. The calculation of the CRC for the JPEG image file requires a routine which can calculate a CRC-32 on a given block of data using a given 32-bit seed value. The initial seed value is set to the image CRC value. (Step 800.) The file is read sequentially and the position of the APP8 is determined and read. (Step 802.) If the APP8 marker cannot be found and read (step 804), an error is returned. (Step 805.) A CRC-32 is calculated for the secure data string within the APP8 data area or block. (Step 806.) The resulting CRC is transformed into CRC' by means of the proprietary transformation technique. (Step 808.) The transformed date CRC' is stored within the image file. (Step 810.)

The present invention has been illustrated and described with respect to specific embodiments thereof. It is to be understood, however, that the above-described embodiments are merely illustrative of the principles of the invention and are not intended to be exclusive embodiments. To facilitate discussion of the present invention, paper document originals (e.g., paper, photos, etc.) which are scanned into digital images are presumed in the DocSTAR embodiment of the present invention. However, it should be understood by one skilled in the art, that the present invention will be equally applicable to any digital file regardless of its source or how it is generated, for example, digital images originating from digital cameras, medical imaging devices, word processing or spreadsheet applications or other sources.

Alternative embodiments capturing variations in the enumerated embodiments disclosed herein can be implemented to achieve the benefits of the present invention.

It should further be understood that the foregoing and many various modifications, omissions and additions may be devised by one skilled in the art without departing from the spirit and scope of the invention.

It is therefore intended that the present invention is not limited to the disclosed embodiments but should be defined in accordance with the claims which follow.

I claim:

CLAIMS

1. A digital file management and imaging system comprising:

means for inputting a digital file;

a secure date and time reference providing date and time information;

means for generating a date/time value derived from said date and time information;

means for generating an image value derived from said digital file;

means for marking said digital file with said date and time information, said date/time value and said image value; and

means for storing said marked digital file.

2. The system of claim 1 wherein said secure date and time reference is a local secure clock.

3. The system of claim 1 wherein said means for generating the date and time value implements a cyclic redundancy code algorithm.

4. The system of claim 1 wherein said means for generating the image value implements a cyclic redundancy code algorithm.

5. The system of claim 1 further including means for transforming the date/time value and said means for marking marks the digital file with the transformed date/time value.

6. The system of claim 5 wherein the means for transforming the date/time value implement a mathematical transformation.

7. The system of claim 1 further including means for transforming the image value and said means for marking marks the digital file with the transformed image value.

8. The system of claim 7 wherein the means for transforming the image value implement a mathematical transformation.

9. The system of claim 1 wherein the digital file is an image file.

10. The system of claim 1 wherein the digital file is a text file.

11. The system of claim 1 wherein the digital file is a file from a digital camera.

12. The system of claim 1 wherein the digital file is from a medical imaging device.

13. The system of claim 1 wherein the digital file is a computer application generated file.

14. The system of claim 1 further including means for validating a marked file.

15. A digital file management system comprising:

a digital file;

a secure date and time reference providing date and time information;

a date/time value derived from said date and time information;

an image value derived from said digital file;

a marked digital file marked with said date and time information, said date/time value and said image value.

16. The system of claim 15 wherein said secure date and time reference is a local secure clock.

17. The system of claim 15 wherein the date and time value is derived by a cyclic redundancy code algorithm.

18. The system of claim 15 wherein the image value is derived by a cyclic redundancy code algorithm.

19. The system of claim 15 further including a transformed date/time value and said marked file is marked with the transformed date/time value.

20. The system of claim 15 further including a transformed image value and said marked file is marked with the transformed image value.

21. The system of claim 15 wherein the digital file is an image file.

22. The system of claim 15 wherein the digital file is a text file.

23. The system of claim 15 wherein the digital file is a file from a digital camera.

24. The system of claim 15 wherein the digital file is from a medical imaging device.

25. The system of claim 15 wherein the digital file is a computer application generated file.

26. A method of digital file management and imaging comprising the steps of:

providing a digital file;

providing date and time information from a secure date and time reference from a local source;

generating a date/time value derived from said date and time reference;

generating an image value derived from said digital file;

marking said digital file with said date and time information, said date/time value and said image value; and

storing said marked digital file.

27. The method of claim 26 wherein said step of generating the data and time value implements a cyclic redundancy code algorithm.

28. The method of claim 26 wherein said means for generating the image value implements a cyclic redundancy code algorithm.

29. The method of claim 26 further including the step of transforming the date and time value and marking the digital file with the transformed date and time value.

30. The method of claim 26 further including the step of transforming the image value and marking the digital file with the transformed date and time value.

31. The method of claim 26 wherein said step for providing a digital file includes optically scanning an original image into a digital image.

32. The method of claim 26 further including recalculating the date/time value and image value and comparing the recalculated values to the date/time and image values respectively which are marked in the image.

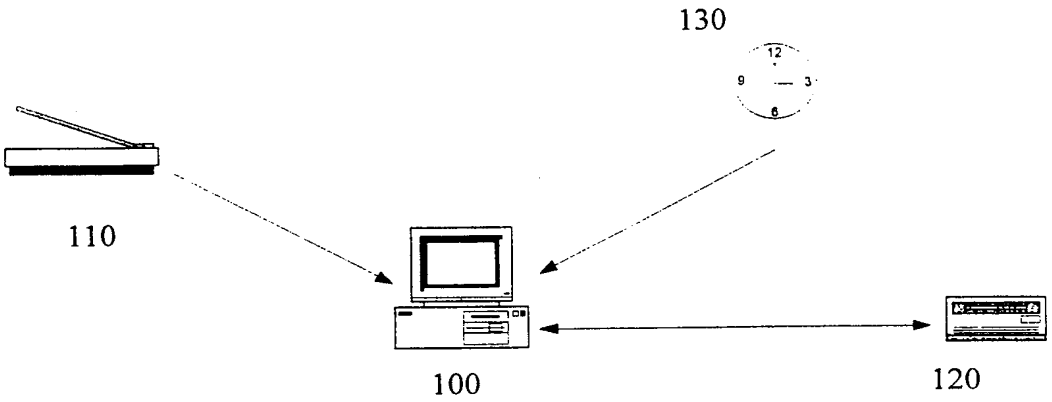


FIG. 1

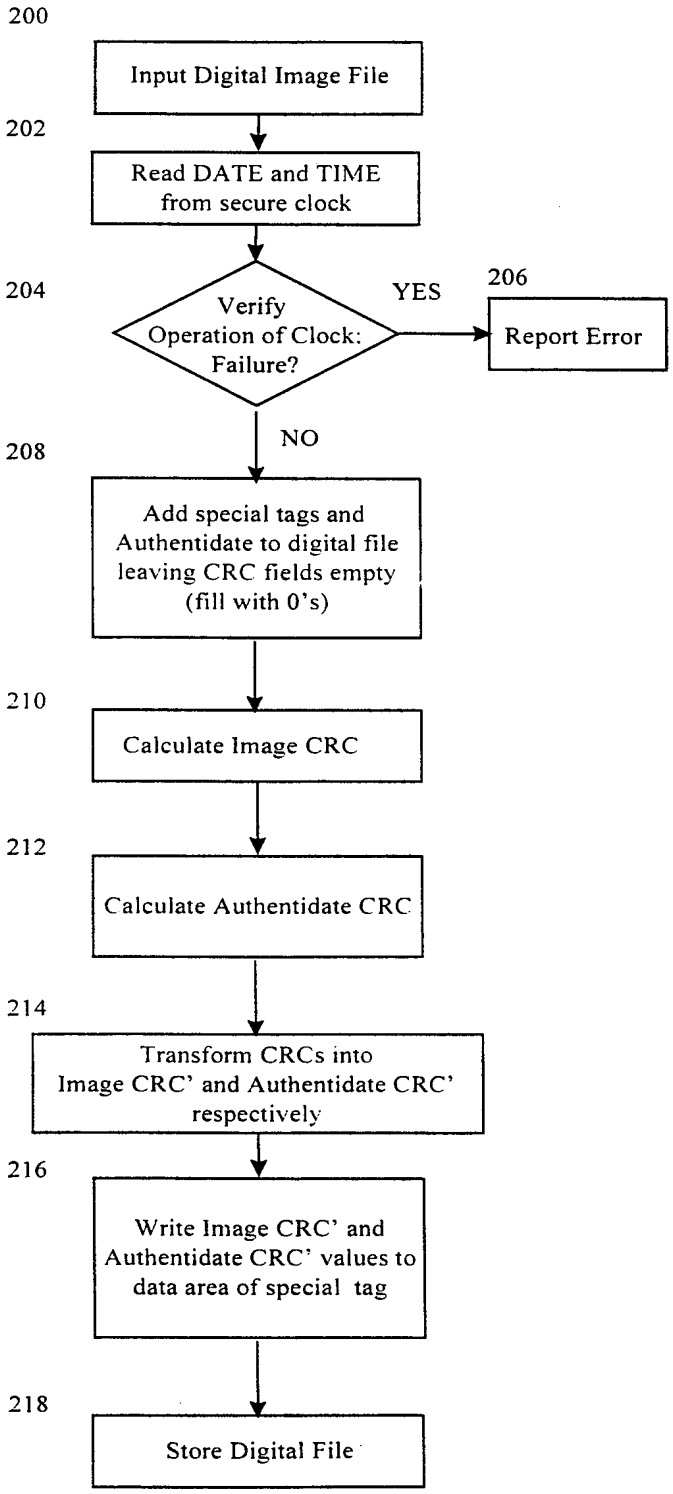

200
Input Digital Image File
202
Read DATE and TIME from secure clock
204
Verify Operation of Clock: Failure?
YES
206
Report Error
NO
208
Add special tags and Authentidate to digital file leaving CRC fields empty (fill with 0's)
210
Calculate Image CRC
212
Calculate Authentidate CRC
214
Transform CRCs into Image CRC' and Authentidate CRC' respectively
216
Write Image CRC' and Authentidate CRC' values to data area of special tag
218
Store Digital File

FIG. 2

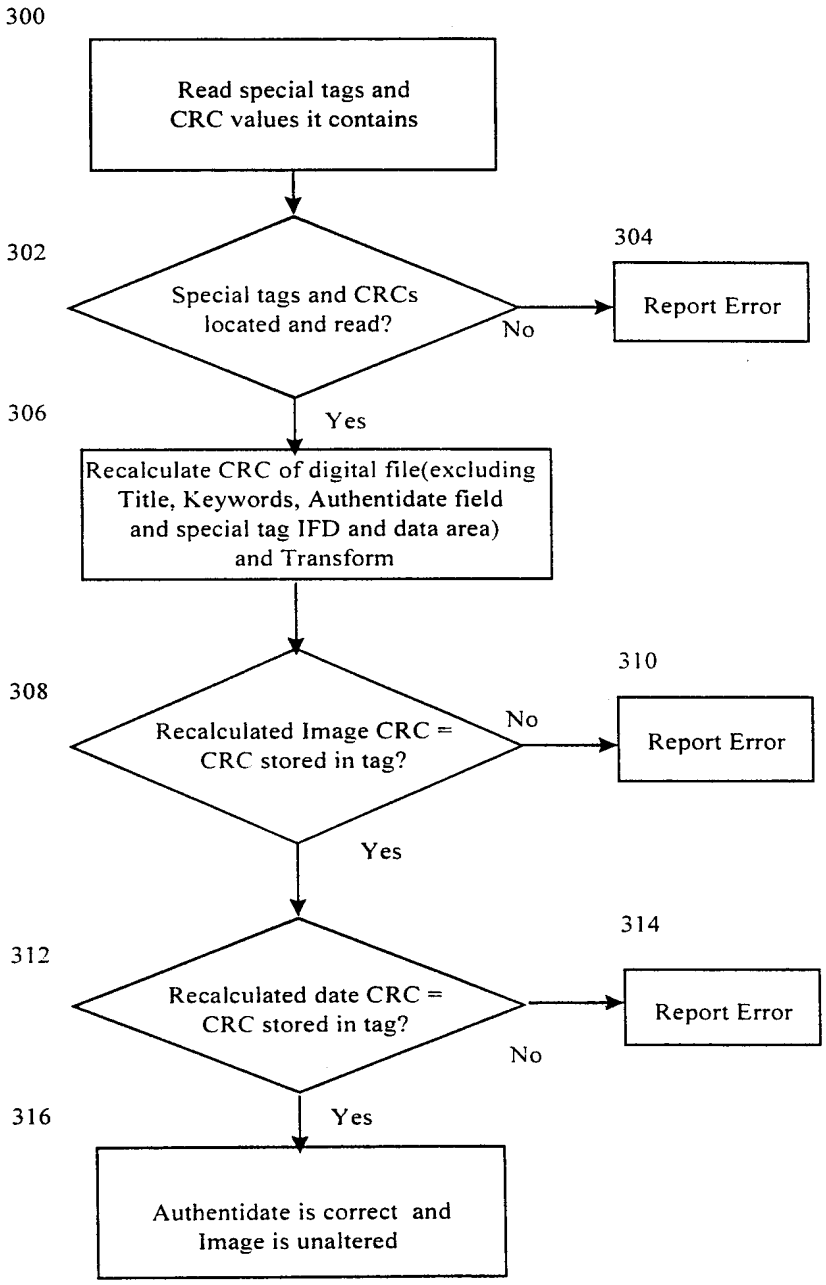

300
Read special tags and CRC values it contains
302
Special tags and CRCs located and read?
No
304
Report Error
Yes
306
Recalculate CRC of digital file(excluding Title, Keywords, Authentidate field and special tag IFD and data area) and Transform
308
Recalculated Image CRC = CRC stored in tag?
No
310
Report Error
Yes
312
Recalculated date CRC = CRC stored in tag?
No
314
Report Error
Yes
316
Authentidate is correct and Image is unaltered

FIG. 3

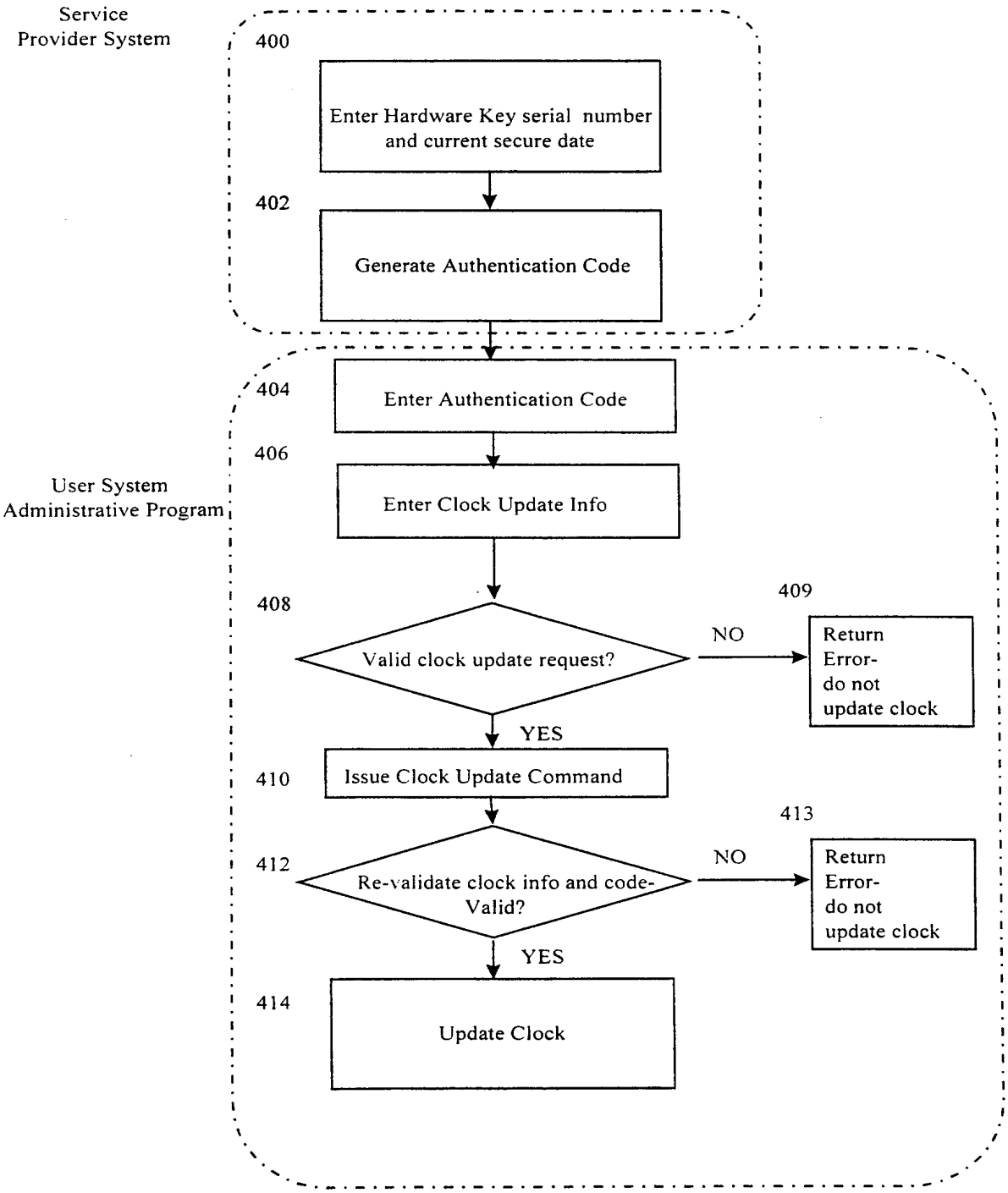

Service Provider System
400
Enter Hardware Key serial number and current secure date
402
Generate Authentication Code
User System Administrative Program
404
Enter Authentication Code
406
Enter Clock Update Info
408
Valid clock update request?
NO
409
Return Error- do not update clock
YES
410
Issue Clock Update Command
412
Re-validate clock info and code- Valid?
NO
413
Return Error- do not update clock
YES
414
Update Clock

FIG. 4

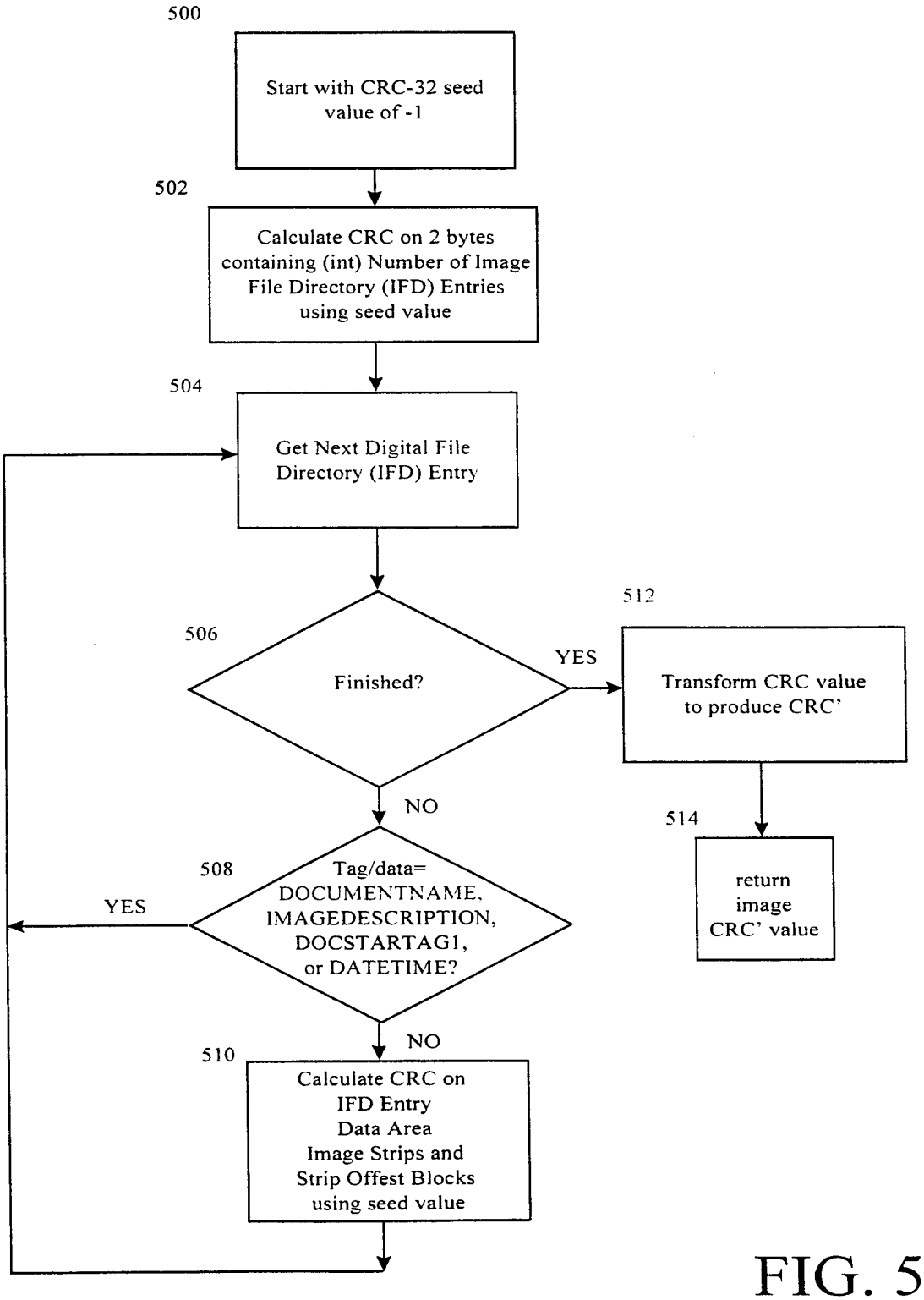

500
Start with CRC-32 seed value of -1
502
Calculate CRC on 2 bytes containing (int) Number of Image File Directory (IFD) Entries using seed value
504
Get Next Digital File Directory (IFD) Entry
506
Finished?
YES
512
Transform CRC value to produce CRC'
514
return image CRC' value
NO
508
Tag/data= DOCUMENTNAME, IMAGEDESCRIPTION, DOCSTARTAG1, or DATETIME?
YES
NO
510
Calculate CRC on IFD Entry Data Area Image Strips and Strip Offest Blocks using seed value

FIG. 5

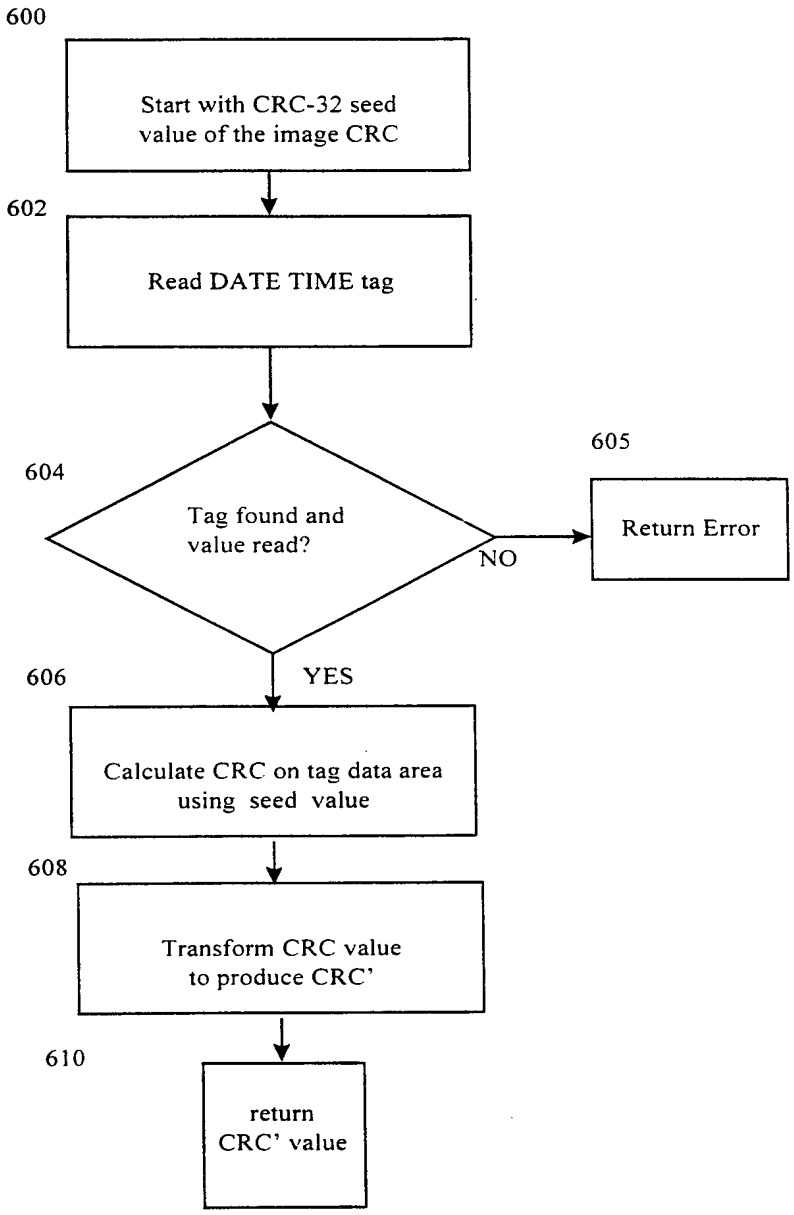

600
Start with CRC-32 seed value of the image CRC
602
Read DATE TIME tag
604
Tag found and value read?
NO
605
Return Error
YES
606
Calculate CRC on tag data area using seed value
608
Transform CRC value to produce CRC'
610
return CRC' value

FIG. 6

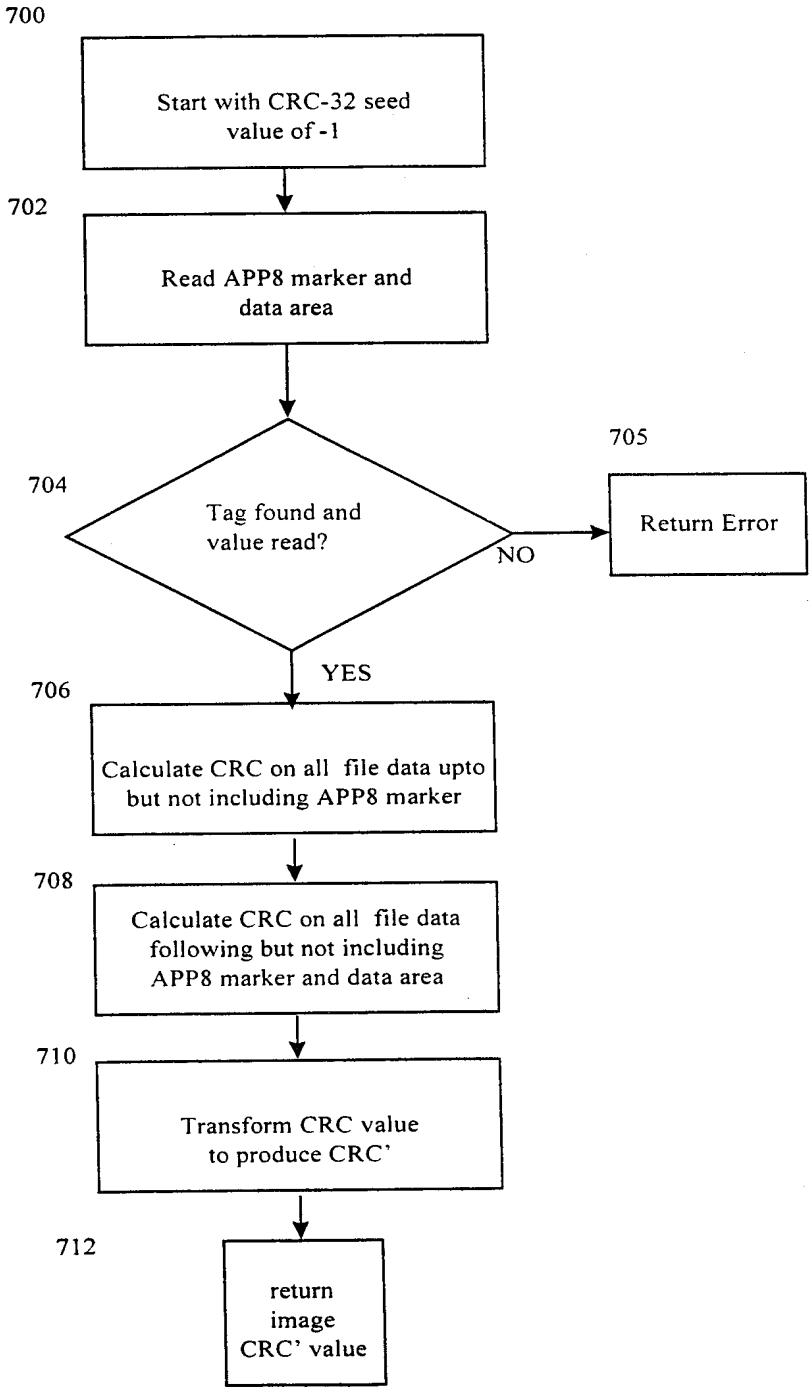

700
Start with CRC-32 seed value of -1
702
Read APP8 marker and data area
704
Tag found and value read?
NO
705
Return Error
YES
706
Calculate CRC on all file data upto but not including APP8 marker
708
Calculate CRC on all file data following but not including APP8 marker and data area
710
Transform CRC value to produce CRC'
712
return image CRC' value

FIG. 7

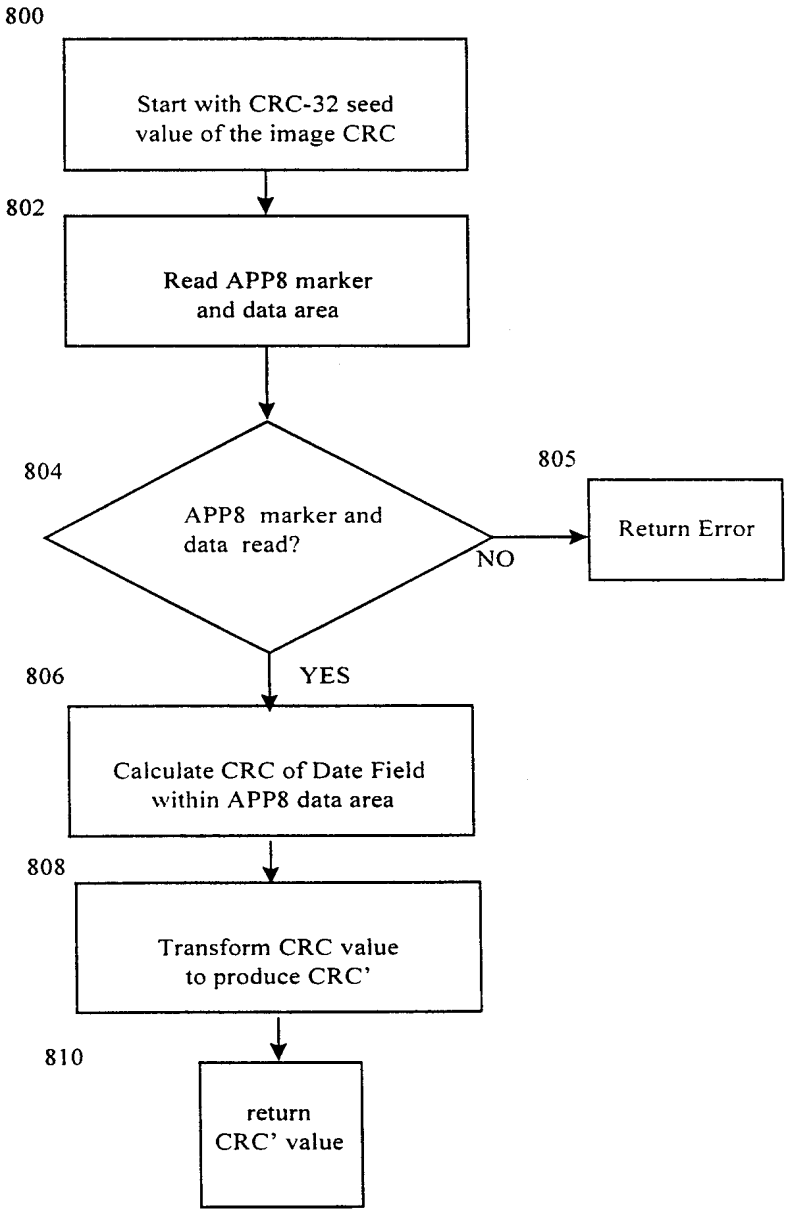

800
Start with CRC-32 seed value of the image CRC
802
Read APP8 marker and data area
804
APP8 marker and data read?
NO
805
Return Error
YES
806
Calculate CRC of Date Field within APP8 data area
808
Transform CRC value to produce CRC'
810
return CRC' value

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05098

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/08
US CL : 380/4, 54
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4, 54, 3, 5; 707/104

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NPL, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,875,249 A (MINTZER et al) 23 February 1999, see the abstract, Figure 1, column 1, lines 5-7, column 2, lines 33-38, column 3, lines 25-60	1-32
Y, P	US 5,949,879 A (BERSON et al) 07 September 1999, see the abstract, Figure 1.	1-32
Y	US 5,499,294 A (FRIEDMAN) 12 March 1996, see the abstract.	11, 23
Y	US 5,870,471 A (WOOTTON et al) 09 February 1999, see column 1, lines 39-50.	12, 24
Y, P	US 5,923,763 A (WALKER et al) 13 July 1999, see column 5, lines 34-45.	3, 4, 6, 8, 17, 18, 27, 28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
20 MAY 2000

Date of mailing of the international search report
12 JUN 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
UYEN LE
Telephone No. (703) 305-4134

Form PCT/ISA/210 (second sheet) (July 1998) ★